WHAT IS CLAIMED IS:

1. An e-mail message transmission system, which cooperates with a remote publicly accessible security server to securely transmit e-mail messages, comprising:

a security manager, the security manager encrypting an e-mail message in accordance with encryption data;

a lookup module associated with the security manager, the lookup module querying the remote security server for encryption data, the lookup module identifying at least one target server for a e-mail message, the lookup module automatically retrieving encryption data for the identified target server by submitting a corresponding request to the remote server; and

a transmission module, the transmission module transmitting the e-mail message to at least one target server for which encryption data was retrieved by the lookup module.

2. The system of Claim 1, further comprising a policy manager, the policy manager enforcing policy to facilitate the identification of encryption data to be employed in encrypting the e-mail message by the security manager.

3. The system of Claim 1, wherein the policy manager provides an encryption data preference indicator by referring to at least the semantic content of the e-mail message and stored policy information.

4. An e-mail message transmission system, comprising:

a first e-mail firewall, the first e-mail firewall associated with a first plurality of user computers, the first e-mail firewall coupled to a public wide area network by a first network connection;

a second e-mail firewall, the second e-mail firewall associated with a second plurality of user computers, the second e-mail firewall coupled to the public wide area network by a second network connection; and

a security data lookup server, the security data lookup server storing security data for at least the first e-mail firewall and the second e-mail firewall, the security data lookup server coupled to the public wide area network by a third network connection, whereby the first e-mail firewall transmit a request for security data to the security data lookup server so as to receive security data corresponding to the second e-mail firewall and facilitate a secure public network between the first e-mail firewall and the second e-mail firewall.

5. The system of Claim 4, wherein the security data is public key encryption certificate data.

6. The system of Claim 4, wherein the public wide area network is the Internet.

7. An e-mail message transmission method, comprising:

receiving an e-mail message into a transmission server, the e-mail message associated with at least one recipient server, the recipient server is coupled to the transmission server by a network connection;

accessing a lookup server to retrieve encryption data corresponding to at least the recipient server, the lookup server is coupled to the transmission server by a network connection;

encrypting the e-mail message in accordance with the retrieved encryption data; and

transmitting the encrypted e-mail message to the recipient server.

8. An e-mail message reception method, comprising:

receiving an encrypted e-mail message from a remote server;

decrypting the e-mail message in accordance with encryption data;

extracting signature data from the e-mail message;

verifying the extracted signature data by accessing a signature verification server; and

processing the e-mail message in accordance with said verifying.

9. The method of Claim 8, further comprising employing a policy to determine whether the e-mail message signature should be verified.

10. The method of Claim 8, further comprising employing a policy to determine the requirements for verification of signature data.

11. An e-mail message transmission system, comprising:

means for receiving an e-mail message, the e-mail message including at least one recipient identifier;

means for identifying a remote certificate server corresponding to a target e-mail server associated with said at least one recipient identifier;

means for querying said identified remote server for encryption data corresponding to the target e-mail server;

means for encrypting said e-mail message in accordance with said encryption data from said remote server; and

means for transmitting said encrypted e-mail message to said remote server.

12. The system of Claim 11, further comprising means for applying a security policy to the e-mail message, the security policy results employed by said means for identifying and said means for querying.

13. A method for signing an e-mail message, comprising:

receiving an e-mail message by a security manager of an e-mail firewall;

determining if a signature is required for the received e-mail message by applying a signature policy;

retrieving a signing certificate for the message by applying a signature policy;

applying the retrieved signing certificate to the message; and

forwarding the message for further processing by the e-mail firewall.

14. The method of Claim 13 wherein said determining if a signature is required for the message is by applying a first signature policy and said retrieving of a signature is by reference to a second signature policy.

15. The method of Claim 13 wherein said determining and said retrieving is by reference to applying of one signature policy.